UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/660,263	09/10/2003	Benedicto H. Dominguez	VISAP073/P-13100	5063

75458 7590 07/03/2008

Beyer Law Group LLP/Visa
P.O. BOX 1687
Cupertino, CA 95015-1687

EXAMINER	
KUCAB, JAMIE R	

ART UNIT	PAPER NUMBER
3621	

MAIL DATE	DELIVERY MODE
07/03/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 10/660,263
Filing Date: September 10, 2003
Appellant(s): DOMINGUEZ ET AL.

Laura M. Dean
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed April 14, 2008 appealing from the Office action mailed November 14, 2007.

(1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The following are the related appeals, interferences, and judicial proceedings known to the examiner which may be related to, directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal:

One or more appeal briefs were filed in at least one of the patent applications cross-referenced in the present application. However, none of these appeals were allowed to reach the stage of being decided by the board.

An interference was requested in patent application 10/384,735, which is in the same family as one of the applications cross-referenced in the present patent application. However, while the claims upon which the interference was requested remain pending, an interference has not been granted as of this time.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct. This appeal involves claims 1-7, 9-18, 20-21, 23-37, 39-41, 44-47, 49-50, and 52-54.

(4) Status of Amendments After Final

The appellant's statement of the status of amendments after final rejection contained in the brief is correct.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct. Additionally, the following new grounds of rejection is being added:

NEW GROUNDS OF REJECTION

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claims 1-7, 9-18, 20, 21, 23, 24, 37, 39-41, 44-47, 49, and 50 are rejected under 35 U.S.C. §101, because the claimed invention is directed to non-statutory subject matter. Based on Supreme Court precedent, and recent Federal Circuit decisions, a § 101 process must (1) be tied to another statutory class (such as a particular apparatus) or (2) transform underlying subject matter (such as an article or materials) to a different state or thing. *Diamond v. Diehr*, 450 U.S. 175, 184 (1981); *Parker v. Flook*, 437 U.S. 584, 588 n.9 (1978); *Gottschalk v. Benson*, 409 U.S. 63, 70 (1972); *Cochrane v. Deener*, 94 U.S. 780,787-88 (1876). The process steps in claims 1-7, 9-18, 20, 21, 23, 24, 37, 39-41, 44-47, 49, and 50 are not tied to another statutory class nor do they execute a transformation. Thus, they are non-statutory.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

6,839,692	CARROTT	01-2005
2004/0083184	TSUEI	04-2004

(9) Grounds of Rejection

The following grounds of rejection are applicable to the appealed claims:

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claims 1-7, 9-18, 20, 21, 23, 24, 37, 39-41, 44-47, 49, and 50 are rejected under 35 U.S.C. §101, because the claimed invention is directed to non-statutory subject matter. Based on Supreme Court precedent, and recent Federal Circuit decisions, a § 101 process must (1) be tied to another statutory class (such as a particular apparatus) or (2) transform underlying subject matter (such as an article or materials) to a different state or thing. *Diamond v. Diehr*, 450 U.S. 175, 184 (1981); *Parker v. Flook*, 437 U.S. 584, 588 n.9 (1978); *Gottschalk v. Benson*, 409 U.S. 63, 70 (1972); *Cochrane v. Deener*, 94 U.S. 780,787-88 (1876). The process steps in claims (1-7, 9-18, 20, 21, 23, 24, 37, 39-41, 44-47, 49, and 50) are not tied to another statutory class nor do they execute a transformation. Thus, they are non-statutory.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-7, 9-18, 20, 21, 23-37, 39-41, 44-47, 49, 50, and 52-54 are rejected under 35 U.S.C. §103(a) as being unpatentable over Carrott et al. (hereinafter Carrott, 6,839,692 B2), in view of Tsuei et al. (hereinafter Tsuei, US 2004/0083184 A1).

As per claims 1-3, 6, 7, 37 and 41, Carrott discloses a method involving a presenter, a trusted party, and an acceptor for validating profile data of said presenter during an on-line transaction comprising: receiving said profile data at said trusted party (Col. 2, lines 5-10; Col. 3, lines 4-10; Col. 4, lines 8-18; Col. 5, lines 25-38 and 55-67; Col. 6, lines 60-65); receiving and comparing said profile data against reference data stored by said trusted party (Col. 2, lines 5-10 and 20-33; Col. 3, lines 4-10; Col. 7, lines 4-10 and 17-25); notifying said acceptor by said trusted party that said profile data of said presenter is either authentic or erroneous, whereby said trusted party validates said profile data of said presenter for the benefit of said acceptor (Col. 2, lines 5-10 and 20-33; Col. 7, lines 24-42).

Carrott does not explicitly disclose receiving by said trusted party an enrollment process (see background of the invention), profile data and enrollment data from said presenter and verifying the identity of said presenter, said trusted party being an issuer of an account to said

presenter wherein authentication data is received and validated as per the customer profile during an online transaction.

Tsuei, however, teaches a dynamic and comprehensive system and method for processing and authentication of transactions via identified customer profiles without revealing any information the requesting party (see figure 2 and associated text, ¶14, 17 19, 25, 66). According to Tsuei, once a subscriber enrolls and registers providing profile and enrollment data, a unique identifier is associated with that customer, upon matching such data and verification of the identity and credentials of the customer, notification is provided for the benefit of the requesting party over the Internet (summary of the invention, fig 2 and associated text, ¶14, 17, 19, 70-74, 89-114; also see 158-160, creation of vault database). Therefore, it would have been obvious for one of ordinary skill in the art at the time of the invention to modify Carrot's purchase transaction system to provide an anonymous transaction verification mechanism to provide security to the subscriber while at the at the same time providing further verification confirmation for the requestor.

Furthermore, Carrott does not explicitly disclose communicating said authentication data between said trusted party and said presenter during said enrollment process, said authentication data being known only to said trusted party and to said presenter.

Tsuei teaches that HPS 118 uses a standard credit card authorization system. However, the issuer must establish a method for authenticating the cardholder of an alias account. In an embodiment of the invention, this is accomplished by using the alias "password" that was entered during account setup. The issuer should also have some special procedures to handle referrals and hot calls. Since none of the information on the alias account is real, a phone number

is set in the phone number field that will allow the issuer to communicate with the vault and request contact with the cardholder [0139]. Therefore, it would have been obvious to one of ordinary skill in the art to modify Carrott to include assigning a password during the enrollment process that is known to the user and sent to the trusted party to authenticate communication between the parties.

As per claims 4 and 5, Carrott further discloses wherein the presenter and the acceptor communicate with said trusted party over the Internet (Abstract; Figure 1; Col. 3, lines 45-55; Col. 8, lines 10-15).

As per claims 9, 10, 44, 45, Carrot fails to disclose as noted above, however, Tsuei teaches a system wherein the program identity is an account number of financial account wherein the trusted third party maintains said account (fig 12-17, 20 and associated text). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to modify the method of Carrott et al and include a program identity number such as an account number, unique identifier or other code of some sort issued and stored by the trusted party so that the trusted party has a unique number or code associated with the presenter as taught by Tsuei et al and which may be used later to identify the presenter or an account maintained by the trusted party.

As per claims 11-12 and 14-17, Carrott et al further disclose initiating communications between the presenter and acceptor and receiving profile data and a program identity number at the acceptor for the presenter (Col. 4, lines 5-18; Col. 5, lines 25-38). Carrott et al, however, fail to explicitly disclose receiving identity data at the acceptor. Tsuei et al disclose a method for verifying the identity of on-line credit card purchasers and further teach receiving, at a trusted

party, authenticating data from the presenter; comparing, by the trusted party, the authenticating data against pre-designated authenticating data previously designated for the presenter and notifying the acceptor by the trusted party that the identity of the presenter is either authentic or erroneous, whereby the trusted party authenticates the identity of the presenter for the benefit of the acceptor (fig 2, 12-20 and associated text, ¶12-30, 70-158). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to modify the method of Carrott et al and include authenticating the identity of the purchaser as taught by Tsuei et al so that the merchant is ensured that the purchaser is the authorized user for the credit card. Tsuei et al provides motivation by indicating that there is a need for a method or system for verifying the identity of an on-line purchaser, and ensuring to a reasonable extent that the purchaser is in fact the party authorized to use the credit card presented for payment.

As per claim 13, Carrott et al further disclose querying the trusted party by the acceptor whether account data updating can be provided (Col. 2, lines 25-33).

As per claims 18 and 20-21, Carrott et al further disclose transmitting a data authentication request message from said acceptor to said trusted party in order to request that said trusted party validate said profile data of said presenter as discussed above. Carrott et al, however, fail to disclose requesting that the third party authenticate the identity of the presenter. Tsuei et al disclose a method for requesting that the trusted party verifying the identity of on-line credit card purchasers and further teach notifying the acceptor that the identity is authentic when the data matches (fig 2, 12-20 and associated text, ¶12-30, 70-158). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to modify the method of Carrott et al and include authenticating the identity of the purchaser as taught by Tsuei et al so

that the merchant is ensured that the purchaser is the authorized user for the credit card. Tsuei et al provides motivation by indicating that there is a need for a method or system for verifying the identity of an on-line purchaser, and ensuring to a reasonable extent that the purchaser is in fact the party authorized to use the credit card presented for payment.

As per claims 23-24, Carrott et al further disclose providing, by the trusted party, of updated profile data when the profile data is determined to be out of date (Col. 2, lines 25-33, see also updating disclosed in Tsuei).

As per claims 25, 27, 52 and 54, Carrott et al disclose an on-line data authentication system comprising: a trusted party who receives, validates and provides profile data of a presenter (Figure 1; Col. 2, lines 5-10 and 20-33; Col. 3, lines 4-10; Col. 4, lines 8-18; Col. 5, lines 25-38 and 55-67; Col. 6, lines 60-65; Col. 7, lines 4-10 and 17-25); an acceptor who conducts a transaction with said presenter and who requests said trusted party to validate said profile data of said presenter (Figure 1; Col. 6, lines 60-67; Col. 7, lines 1-10); and a directory server configured to determine the existence of said trusted party who will be able to validate said profile data of said presenter (Col. 6, lines 60-67; Col. 7, lines 1-10).

Carrott et al further disclose local user authentication wherein the user inputs a user ID and password which is then verified by the users computer prior to proceeding (Col. 5, lines 57-63; Col. 6, lines 20-25). Carrott et al, however, fail to explicitly disclose receiving authentication data at a trusted party during an enrollment process, said trusted party being an issuer of an account to said presenter in which enrollment data is used to verify the identity of said presenter, and an acceptor requesting the trusted party to authenticate the identity of the presenter. Tsuei et al disclose a method for verifying the identity of on-line credit card purchasers and further teach

receiving during an enrollment process, at a trusted party, authenticating data from the presenter; comparing, by the trusted party, the authenticating data against pre-designated authenticating data previously designated for the presenter; and notifying the acceptor by the trusted party that the identity of the presenter is either authentic or erroneous, whereby the trusted party authenticates the identity of the presenter for the benefit of the acceptor (fig 2, 12-20 and associated text, ¶12-30, 70-158). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to modify the method of Carrott et al and include authenticating the identity of the purchaser as taught by Tsuei et al so that the merchant is ensured that the purchaser is the authorized user for the credit card. Tsuei et al provides motivation by indicating that there is a need for a method or system for verifying the identity of an on-line purchaser, and ensuring to a reasonable extent that the purchaser is in fact the party authorized to use the credit card presented for payment.

Furthermore, Carrott does not explicitly disclose communicating said authentication data between said trusted party and said presenter during said enrollment process, said authentication data being known only to said trusted party and to said presenter.

Tsuei teaches that HPS 118 uses a standard credit card authorization system. However, the issuer must establish a method for authenticating the cardholder of an alias account. In an embodiment of the invention, this is accomplished by using the alias "password" that was entered during account setup. The issuer should also have some special procedures to handle referrals and hot calls. Since none of the information on the alias account is real, a phone number is set in the phone number field that will allow the issuer to communicate with the vault and request contact with the cardholder [0139]. Therefore, it would have been obvious to one of

ordinary skill in the art to modify Carrott to include assigning a password during the enrollment process that is known to the user and sent to the trusted party to authenticate communication between the parties.

As per claims 26 and 53, Carrott et al further disclose wherein the presenter and the acceptor communicate with said trusted party over the Internet (Abstract; Figure 1; Col. 3, lines 45-55; Col. 8, lines 10-15).

As per claim 28, Carrott et al fail to disclose as above, however, Tsuei et al disclose receiving and storing authenticating data from the presenter at the trusted party wherein the authenticating data becomes the pre-designated authenticating data (fig 2, 12-20 and associated text, ¶12-30, 70-158). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to modify the method of Carrott et al and include receiving and storing, at the trusted party, authenticating data of the purchaser as pre-designated authenticating data for purposes of authenticating the identity of the purchaser as taught by Tsuei et al so that the merchant is ensured that the purchaser is the authorized user for the credit card. Tsuei et al provides motivation by indicating that there is a need for a method or system for verifying the identity of an on-line purchaser, and ensuring to a reasonable extent that the purchaser is in fact the party authorized to use the credit card presented for payment.

As per claims 29-30, Carrott et al fail to disclose, however, Tsuei et al disclose providing, by the trusted party, to the presenter a program identity number which is correlated with the identity, profile data and authenticating data and storing the program identity number by the trusted party (fig 2, 12-20 and associated text, ¶12-30, 70-158). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to modify the method of

Carrott et al and include a program identity number such as an account number, unique identifier or other code of some sort issued and stored by the trusted party so that the trusted party has a unique number or code associated with the presenter as taught by Tsuei et al and which may be used later to identify the presenter or an account maintained by the trusted party.

As per claims 31-32, Carrott et al disclose a request message transmitted from the acceptor to the trusted party via a directory server, the message containing a query as to whether the trusted party will be able to validate the profile data of the presenter (Col. 6, lines 45-67) and a response message for validating the profile data of the presenter (Col. 2, lines 5-10 and 20-33; Col. 7, lines 24-42). Carrott et al, however, fail to disclose transmitting a message to the third party querying the third party as to whether the third party will be able to authenticate the identity of the presenter. Tsuei et al disclose a method for requesting that the trusted party verifying the identity of on-line credit card purchasers and further teach notifying the acceptor that the identity is authentic when the data matches (fig 2, 12-20 and associated text, ¶12-30, 70-158). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to modify the method of Carrott et al and include authenticating the identity of the purchaser as taught by Tsuei et al so that the merchant is ensured that the purchaser is the authorized user for the credit card. Tsuei et al provides motivation by indicating that there is a need for a method or system for verifying the identity of an on-line purchaser, and ensuring to a reasonable extent that the purchaser is in fact the party authorized to use the credit card presented for payment.

As per claims 33-36, Carrott et al disclose a request message transmitted from the acceptor to the trusted party via a directory server, the message requesting that the trusted party

validate the profile data of the presenter, the request message including profile data of the presenter (Col. 2, lines 5-10; Col. 3, lines 4-10; Col. 4, lines 8-18; Col. 5, lines 25-38 and 55-67; Col. 6, lines 60-65) and a response message for validating the profile data of the presenter and whether or not the profile data is accurate or contains errors (Col. 2, lines 5-10 and 20-33; Col. 7, lines 24-42). Carrott et al, however, fail to disclose transmitting a message to the third party requesting that the third party authenticate the identity of the presenter. Tsuei et al disclose a method for requesting that the trusted party verifying the identity of on-line credit card purchasers and further teach notifying the acceptor that the identity is authentic when the data matches (fig 2, 12-20 and associated text, ¶12-30, 70-158). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to modify the method of Carrott et al and include authenticating the identity of the purchaser as taught by Tsuei et al so that the merchant is ensured that the purchaser is the authorized user for the credit card. Tsuei et al provides motivation by indicating that there is a need for a method or system for verifying the identity of an on-line purchaser, and ensuring to a reasonable extent that the purchaser is in fact the party authorized to use the credit card presented for payment.

As per claims 39-40, Carrott et al further disclose wherein the presenter, acceptor and trusted party communicate over the Internet (Abstract; Figure 1; Col. 3, lines 45-55; Col. 8, lines 10-15).

As per claim 46, Carrott et al further disclose wherein the identity and profile data include at least the name and address of the presenter (Col. 2, lines 20-33; Col. 5 line 60-Col. 6 line 3; Col. 7, lines 24-34).

As per claims 47 and 50, Carrott et al further disclose transmitting a data authentication request message from said acceptor to said trusted party in order to request that said trusted party provide said profile data of said presenter (Figure 2; Col. 2, lines 20-33; Col. 5 line 60-Col. 6 line 3; Col. 7, lines 24-34); and transmitting a data authentication response message from said trusted party to said acceptor, said data authentication response message containing said profile data of said presenter (Col. 2, lines 20-33; Col. 5 line 60-Col. 6 line 3; Col. 7, lines 24-34).

As per claim 49, Carrott et al fail to disclose the features noted as per claim 37 above and asking the presenter, by the trusted party, for permission to provide the profile data of the presenter to the acceptor. However, Tsuei et al disclose requesting the presenter, by the trusted party, for the authenticating data (fig 2, 12-20 and associated text, ¶12-30, 70-158). Examiner takes Official Notice, however, that utilizing a third party entity to essentially filter customer personal or profile data provided to merchants based on permissions controlled by the customer is well known in the art and it would have been obvious to one of ordinary skill in the art at the time of applicant's invention to modify the reference to Carrott et al and include the ability to filter the information provided to the merchant. One would have been motivated to filter this type of customer personal or profile data since it was well known at the time of applicant's invention that consumers were generally concerned about divulging personal or private information.

(10) Response to Argument

Appellant's Argument

As per claims 1-7, 9-18, 20, 21, 23-37, 39-41, 44-47, 49, 50 and 52-54, Appellant argues that the cited references fail to disclose the limitation that a trusted third party verifies the identity of the presenter "during an enrollment process" (independent claims 1, 25, 37, 52). Appellant appears to agree that identity verification by a trusted third party is disclosed in the references but contends that it does not take place "during an enrollment process."

Examiner's Response

It is the Examiner's position that "an enrollment process" includes not only the initial enrollment as Appellant appears to be arguing but also includes any process of modifying enrollment data by the presenter. By this interpretation, the initial enrollment itself is then just a modification of the enrollment data from no data to whatever identity data is collected during the initial enrollment. As referenced on page 3 of the final rejection mailed 14 November 2007, Tsuei discloses at [0202] that when a presenter (Tsuei's "customer") wishes to modify any enrollment data (Tsuei's "subscription data"), his or her identity must be authenticated:

> In order to modify any subscription data, e.g., name or address, the customer will need to authenticate his identity. The authentication process may use a personal identification number (PIN), password, digital certificate, written signature, or other means of positive identification.

Thus, Tsuei discloses verification of identity by a third party "during an enrollment process."

Examiner's Alternative Response

Alternatively, it is the Examiner's position that verification by a trusted third party "during an enrollment process" is inherently disclosed by Tsuei. During the account setup or initial enrollment process, Tsuei discloses at [0100]:

> The issuer processes the part 1 credit card application 104 as any other application. Credit bureau reports are requested and the account is scored to determine credit eligibility and establish an amount of available credit. If the part 1 credit card application 104 is not approved, the normal letters are sent as with any other credit application. If the application is approved, the primary account is booked on the host processing system (HPS) 118 and a primary credit card 40 is issued to the applicant. Under association regulations the address of the booked account is reported to the Issuers Clearing House (ICS) and the credit bureaus.

The credit bureau reports serve as identity verification by a trusted third party. Additionally, in order to issue a credit card, it is inherent that a credit card company verifies to some extent the identity of an applicant, either by requiring a social security number and/or a signature, or by requiring a phone call from the card applicant's home phone number in order to activate the credit card, or by more thorough methods. Although the method and extent of verification may vary from credit card company to credit card company, some verification must take place. Otherwise, it would be impossible for the credit card company to function profitably. Thus, Tsuei inherently discloses verification of identity by a third party "during an enrollment process."

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

This examiner's answer contains a new ground of rejection set forth in section **(9)** above. Accordingly, appellant must within **TWO MONTHS** from the date of this answer exercise one of the following two options to avoid *sua sponte* **dismissal of the appeal** as to the claims subject to the new ground of rejection:

(1) **Reopen prosecution.** Request that prosecution be reopened before the primary examiner by filing a reply under 37 C.F.R. §1.111 with or without amendment, affidavit or other evidence. Any amendment, affidavit or other evidence must be relevant to the new grounds of rejection. A request that complies with 37 C.F.R. §41.39(b)(1) will be entered and considered. Any request that prosecution be reopened will be treated as a request to withdraw the appeal.

(2) **Maintain appeal.** Request that the appeal be maintained by filing a reply brief as set forth in 37 C.F.R. §41.41. Such a reply brief must address each new ground of rejection as set forth in 37 C.F.R. §41.37(c)(1)(vii) and should be in compliance with the other requirements of 37 C.F.R. §41.37(c). If a reply brief filed pursuant to 37 C.F.R. §41.39(b)(2) is accompanied by any amendment, affidavit or other evidence, it shall be treated as a request that prosecution be reopened before the primary examiner under 37 C.F.R. §41.39(b)(1).

Extensions of time under 37 C.F.R. §1.136(a) are not applicable to the TWO MONTH time period set forth above. See 37 C.F.R. §1.136(b) for extensions of time to reply for patent applications and 37 C.F.R. §1.550(c) for extensions of time to reply for ex parte reexamination proceedings.

Respectfully submitted,

/Jamie Kucab/
Examiner, Art Unit 3621

/Andrew J. Fischer/
Supervisory Patent Examiner, Art Unit 3621

/Vincent Millin/
Appeals Practice Specialist 3600

A Technology Center Director or designee must personally approve the new ground(s) of rejection set forth in section (9) above by signing below:

/Wynn W. Coggins/

Director, TC 3600